Setting up Genesys Multicloud CX Private Edition

Networking overview

9/9/2025

Contents

Learn about the network access types for voice and data traffic, and the network elements involved in their architecture. For Kubernetes cluster related network settings, see Network settings.

Related documentation:

-
-

RSS:

- For private edition

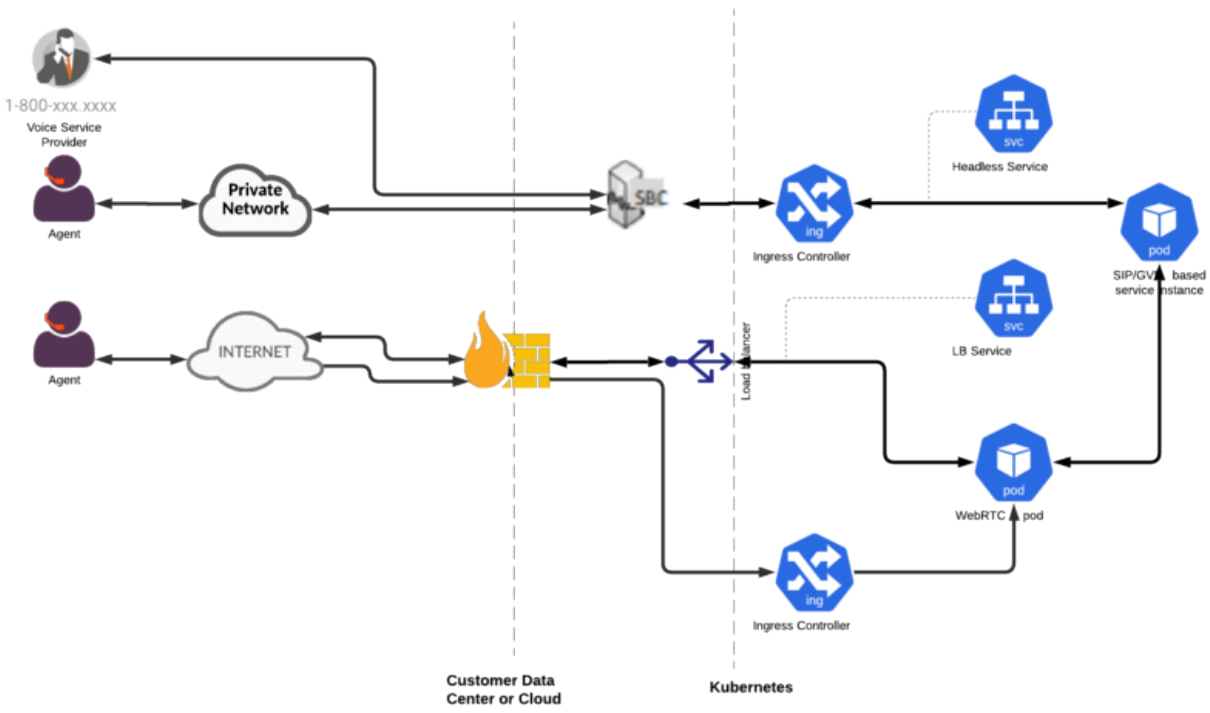
Network access types

There are two types of access to the platform from a tenant perspective:

- **Voice**—Voice (SIP/RTP) traffic
- **Data**—Data traffic.

Voice

The architecture supports SBC integration for both carrier and agent phones, and WebRTC phone access over a data network. The architecture of this voice network is up to you.



Ingress:

- **Firewall for non-HTTP traffic (TCP/UDP)**—Provides network access control (allowlisting, and so on) and a control point for monitoring the traffic.
- Requires VPC or virtual-network native addressing with direct access to the pods IP from SBC.

Data

Your network must include network elements to control the ingress and egress data traffic between the outside world and the Genesys Multicloud CX services running in Kubernetes. However, **you are responsible for determining how to manage access to the Genesys Multicloud CX services**.

The following items are optional, and are shown as examples of how you can control network access.

Ingress:

- **WAF for HTTP and** WebSocket—Provides DDOS protection and being able to terminate TLS at the edge of the network. It is also a control point for monitoring traffic.
- **Firewall for non-HTTP traffic (TCP/UDP)**—Provides network access control (allowlisting, and so on) and a control point for monitoring the traffic.
- **API Gateway**—Enables you to control application and system access to the Genesys Multicloud CX APIs from the standpoint of rate limiting and authorization

Egress:

Implementing Egress is optional and is up to you.

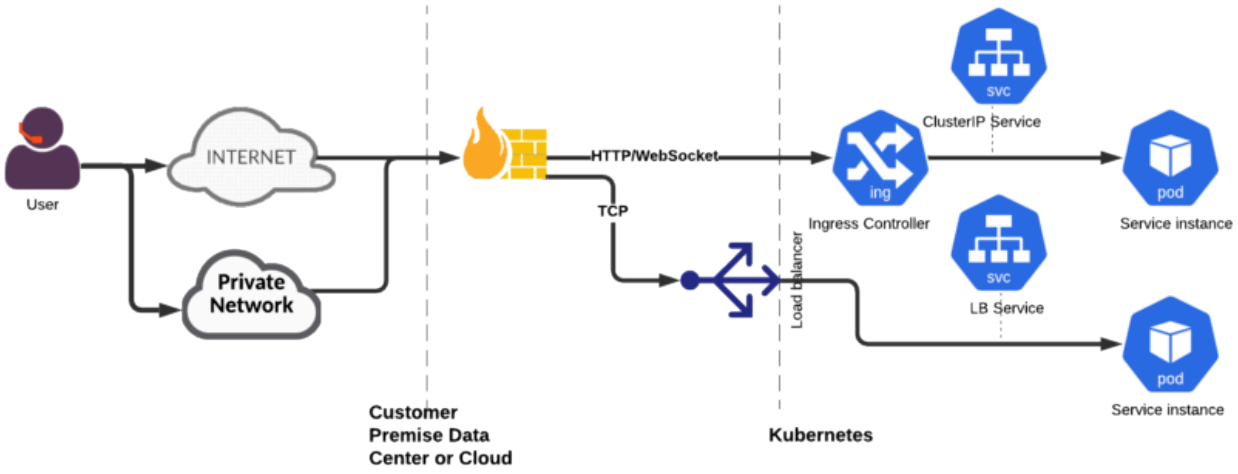
- **Firewall for all external traffic**— Provides network access control (allowlisting, and so on) and a control point for monitoring traffic, to support the security and compliance requirements of your business. All egress traffic to internet destinations must use virtual network-defined or subnet-defined UDR to route traffic through the network firewalls.

Ingress

This architecture uses the following data-related ingress connections:

- HTTP(S)
- WebSocket
- TCP

You must make sure that the right network infrastructure is in place to support your security needs. For more information about the ingress controller and load balancer configurations, see the appropriate service-level guides.

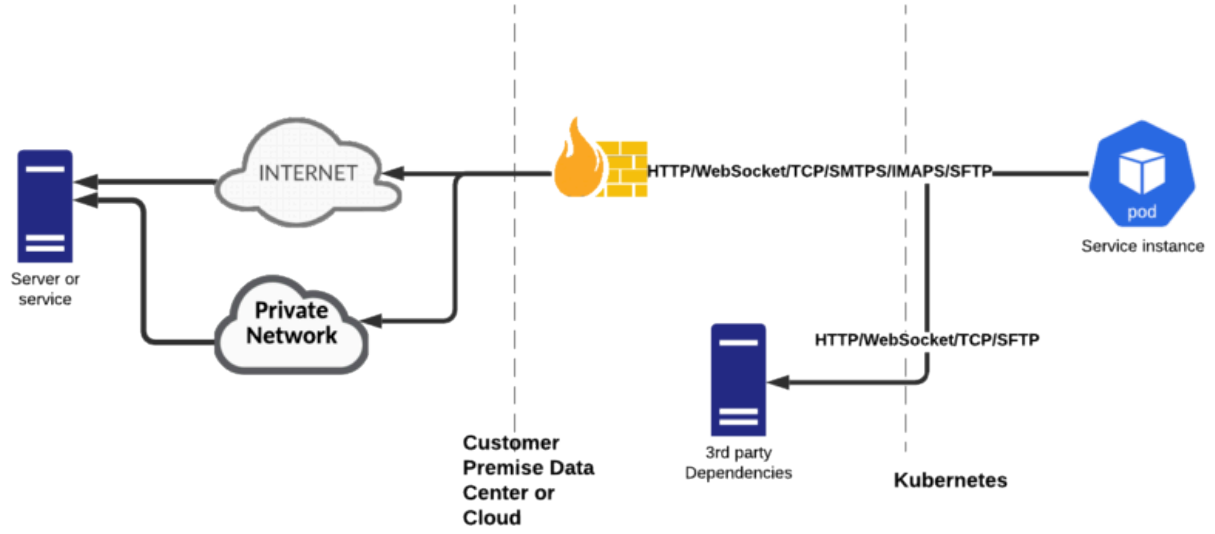


Egress

This architecture uses the following data-related external egress connections:

- HTTPS
- TCP
- SFTP
- IMAPS/SMTPS

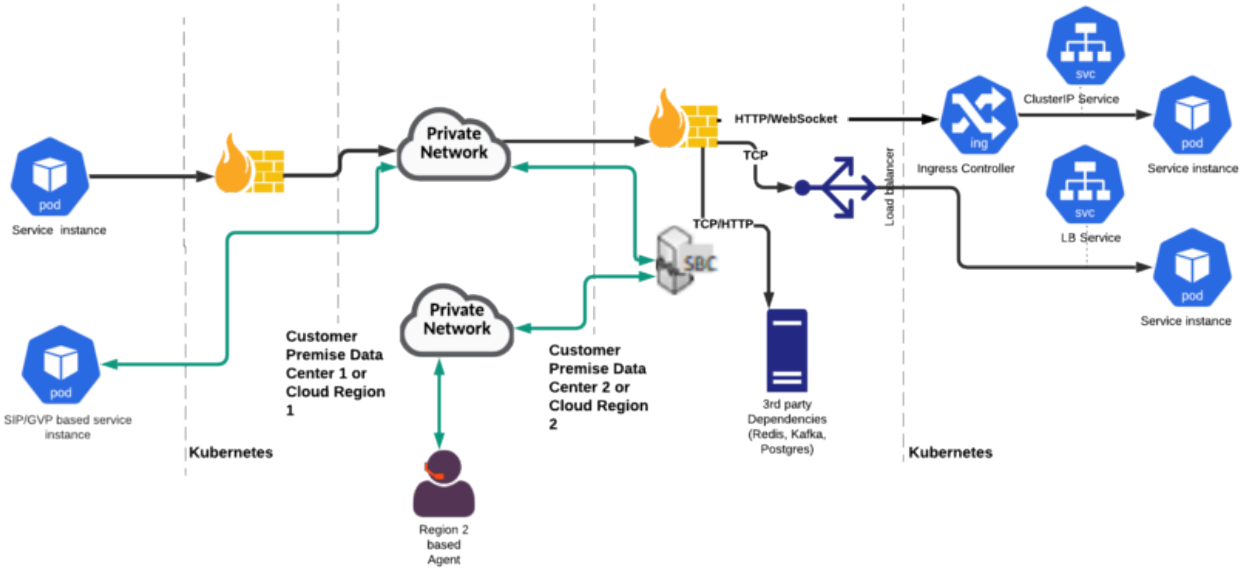
You must make sure that the right network infrastructure is in place to support your security needs.



Cross-Region traffic

This architecture uses the following data-related connections:

- HTTP
- TCP
- SIP/RTP



You must ensure that you have network infrastructure that allows communication between the

following:

- **Regional SBCs**—For optimizing RTP connections when calls are crossing regions
- **Kubernetes clusters**—For Genesys Multicloud CX service-to-service communication
- **Third-party dependency clusters**—For Genesys Multicloud CX services to communicate with the clusters in other regions (such as Kafka, Redis, and Postgres)

The network infrastructure must have the following characteristics:

- **Low latency**—To allow for its use by voice traffic
- **Medium bandwidth**